Save the Sound—that is an umbrella group on both sides of the Long Island Sound—and the Connecticut Fund for the Environment, again, is what really kept the interest level and the pressure on both delegations to make sure that this didn't get lost in the process and allow that mandated sale to move forward.

Mr. Speaker, I strongly urge passage of this bill, and, again, with the gentleman from New York, am determined to make sure that this moves as quickly as possible through the Upper Chamber and is signed into law by President Obama, sending a message to all the individuals and groups that are so interested in preserving Plum Island that, in fact, we, again, have taken it off this sort of conveyor belt and we are going to make sure that it gets the careful treatment that it deserves. At the end of the day, it is going to basically preserve this for generations to come.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, H.R. 1887 has broad bipartisan support. It will ensure that, before DHS disposes of Plum Island, there is a thorough vetting of all the options.

Mr. Speaker, I encourage my colleagues to support this legislation.

I yield back the balance of my time.

□ 1730

Mr. RATCLIFFE. Mr. Speaker, I once again urge my colleagues to support Mr. ZELDIN's bill, H.R. 1887.

I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I rise in support of H.R. 1887, repeals the requirement directing the Administrator of General Services to sell Federal property and assets that support the operations of the Plum Island Animal Disease Center in Plum Island, New York, and for other purposes.

Mr. Speaker, as a senior member of the Homeland Security I support this bill because the safety record of the Plum Island Animal Disease Center is unparalleled.

The Plum Island Animal Disease Center is a United States federal research facility dedicated to the study of animal diseases. It is part of the DHS Directorate for Science and Technology.

Since 1954, the center has had the goal of protecting America's livestock from animal diseases

Throughout the history of the Plum Island Animal Disease Center, there have been no accidental releases of infected animals to the mainland.

The Animal Disease Center on Plum Island has conducted first rate scientific research on a variety of infectious animal-borne diseases, including foot-and-mouth disease, resulting most recently, in the development of a new cell line that rapidly and reliably detects this highly debilitating disease of livestock

Mr. Speaker, in addition to the Animal Disease Center Plum Island contains cultural, historical, ecological, and natural resources of regional and national significance.

Importantly, the Federal Government has invested hundreds of millions of tax payer dollars over the last two decades to make long-term improvements with respect to the conservation and management needs of Long Island Sound and Peconic Bay.

Mr. Speaker, preserving historical and geographical entities play a pivotal role in maintaining homeland security and the sustainability of our ecosystem and health of our community.

I urge all members to join me in voting to pass H.R. 1887.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. RATCLIFFE) that the House suspend the rules and pass the bill, H.R. 1887, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

The title of the bill was amended so as to read: ''A bill to authorize the Comptroller General of the United States to assess a study on the alternatives for the disposition of Plum Island Animal Disease Center, and for other purposes.''.

A motion to reconsider was laid on the table.

NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM ACT OF 2016

Mr. RATCLIFFE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4743) to authorize the Secretary of Homeland Security to establish a National Cybersecurity Preparedness Consortium, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4743

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Cybersecurity Preparedness Consortium Act of 2016''.

SEC. 2. NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM.

(a) IN GENERAL.—The Secretary of Homeland Security may work with a consortium, including the National Cybersecurity Preparedness Consortium, to support efforts to address cybersecurity risks and incidents (as such terms are defined in section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)), including threats of terrorism and acts of terrorism.

(b) ASSISTANCE TO THE NCCIC.—The Secretary of Homeland Security may work with a consortium to assist the national cybersecurity and communications integration center of the Department of Homeland Security (established pursuant to section 227 of the Homeland Security Act of 2002) to—

(1) provide training to State and local first responders and officials specifically for preparing for and responding to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism, in accordance with current law;

(2) develop and update a curriculum utilizing existing programs and models in accordance with such section 227, for State and local first responders and officials, related to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism;

(3) provide technical assistance services to build and sustain capabilities in support of preparedness for and response to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism, in accordance with such section 227;

(4) conduct cross-sector cybersecurity training and simulation exercises for entities, including State and local governments, critical infrastructure owners and operators, and private industry, to encourage community-wide coordination in defending against and responding to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism, in accordance with subsection (c) of section 228 of the Homeland Security Act of 2002 (6 U.S.C. 149);

(5) help States and communities develop cybersecurity information sharing programs, in accordance with section 227 of the Homeland Security Act of 2002, for the dissemination of homeland security information related to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism; and

(6) help incorporate cybersecurity risk and incident prevention and response (including related to threats of terrorism and acts of terrorism) into existing State and local emergency plans, including continuity of operations plans.

(c) PROHIBITION ON DUPLICATION.—In carrying out the functions under subsection (b), the Secretary of Homeland Security shall, to the greatest extent practicable, seek to prevent unnecessary duplication of existing programs or efforts of the Department of Homeland Security.

(d) CONSIDERATIONS REGARDING SELECTION OF A CONSORTIUM.—In selecting a consortium with which to work under this Act, the Secretary of Homeland Security shall take into consideration the following:

(1) Any prior experience conducting cybersecurity training and exercises for State and local entities.

(2) Geographic diversity of the members of any such consortium so as to cover different regions across the United States.

(e) METRICS.—If the Secretary of Homeland Security works with a consortium pursuant to subsection (a), the Secretary shall measure the effectiveness of the activities undertaken by such consortium under this Act.

(f) OUTREACH.—The Secretary of Homeland Security shall conduct outreach to universities and colleges, including historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, and other minority-serving institutions, regarding opportunities to support efforts to address cybersecurity risks and incidents, including threats of terrorism and acts of terrorism, by working with the Secretary pursuant to subsection (a).

(g) TERMINATION.—The authority to carry out this Act shall terminate on the date that is five years after the date of the enactment of this Act.

(h) CONSORTIUM DEFINED.—In this Act, the term ''consortium'' means a group primarily composed of non-profit entities, including academic institutions, that develop, update, and deliver cybersecurity training in support of homeland security.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. RATCLIFFE) and the gentleman from Mississippi (Mr. THOMPSON) each will control 20 minutes.

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. RATCLIFFE. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to

revise and extend their remarks and include any extraneous material on the bill under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Texas?

There was no objection.

Mr. RATCLIFFE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H.R. 4743. The National Cybersecurity Preparedness Consortium Act of 2016 allows the U.S. Department of Homeland Security to work with a consortium, including the National Cybersecurity Preparedness Consortium, to support efforts to address cybersecurity risks and incidents.

This bill allows DHS to engage with a consortium to assist the National Cybersecurity and Communications Integration Center, or NCCIC, in providing training to State and local first responders in preparing for and responding to cybersecurity risks and incidents. An example of a consortium DHS may work with under this bill is the National Cybersecurity Preparedness Consortium, or NCPC.

The NCPC provides State and local communities with the tools they need to prevent, detect, respond to, and recover from cyber attacks. The consortium also evaluates communities' cybersecurity posture and provides them with a roadmap to correct deficiencies in the security of their information systems.

Based out of the University of Texas at San Antonio's Center for Infrastructure Assurance and Security, the NCPC membership includes the University of Arkansas, the University of Memphis, Norwich University, and Texas A&M Engineering Extension Service.

DHS is responsible for carrying out significant aspects of the Federal Government's cybersecurity mission. The Cybersecurity Act, which was recently signed into law, allows DHS to actively share cyber threat indicators and defensive measures with the private sector by affording liability protections.

DHS's National Cybersecurity and Communications Integration Center is responsible for facilitating cross-sector coordination to address cybersecurity risks and incidents.

H.R. 4743 allows DHS to work with any consortium, including the NCPC, in a number of activities, including providing technical assistance, conducting cross-sector cybersecurity training and simulation exercises, and helping States and local communities to develop cybersecurity information sharing programs. Allowing DHS to work with organizations already supporting State and local cyber preparedness and response will provide additional support to State and local entities.

I urge all Members to join me in supporting this bill.

I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield myself such time as I may consume.

I rise in support of H.R. 4743, the National Cybersecurity Preparedness Consortium Act of 2016.

Mr. Speaker, H.R. 4743 allows the Department of Homeland Security to utilize university-based consortia to help provide cybersecurity training and support to State, local, and tribal leaders, including first responders.

There is strong bipartisan support for this legislation, as introduced by the gentleman from Texas (Mr. CASTRO).

H.R. 4743 authorizes DHS to use consortia to provide State and local governments with university-developed cyber training and technical assistance, including for the development of cyber information sharing that jurisdictions in need can use.

Recent studies reveal that organizations at the State and local level describe their cybersecurity programs as being in the early and middle stages of maturity, and 86 percent of State and local respondents identified managing cybersecurity risk as one of their most stressful jobs.

By partnering with consortia, DHS can make a meaningful impact on raising the levels of cybersecurity on the State, local, and tribal levels.

Importantly, H.R. 4743 requires DHS, when selecting a consortium for participation in its cyber efforts, to not only take into account the prior experience of the institutions that would be conducting cybersecurity training exercises, but also the geographic diversity of the institutions participating in the consortium. The inclusion of geographic diversity should help reach more States and localities.

Moreover, I am pleased that the bill requires DHS to do outreach to colleges and universities, including Historically Black Colleges and Universities, Hispanic-serving institutions, and other minority-serving institutions about opportunities to provide research-based cybersecurity-related training exercises and technical assistance.

Mr. Speaker, States and localities need the ability to prevent, detect, respond to, and recover from cyber events as they would have any other disaster or emergency situation. For this reason, I support H.R. 4743 and urge passage.

I reserve the balance of my time.

Mr. RATCLIFFE. Mr. Speaker, I yield 3 minutes to the gentleman from Texas (Mr. HURD), my distinguished friend and colleague.

Mr. HURD of Texas. Mr. Speaker, I thank the gentleman for his leadership on this issue and for yielding me some time.

I would like to also thank the ranking member and my colleague from San Antonio on this piece of legislation that is so important to our hometown.

It is no secret that cyber attacks are on the rise, and the unfortunate reality is that everyone is vulnerable. The costs of protecting your network and properly training communities on best practices in a digital world can be burdensome.

As we all know, State and local communities, in many instances, do not possess the same digital resources as the Federal Government. States and communities need the ability to detect, respond to, and recover from cyber events just as they would any other disaster or emergency situation.

That is why I am proud to be an original cosponsor of H.R. 4743, which will allow DHS to coordinate with a handful of universities that have been leading the way in cyber preparedness.

One of these universities, the University of Texas at San Antonio, is located in my hometown and serves many of my constituents. Another leader in this field is none other than my alma mater, Texas A&M University.

Building upon their great work and the breakthroughs of others across the country will be crucial to protecting our digital infrastructure at all levels. This will help us ensure that our first responders and government entities are adequately prepared for a significant cyber event.

I thank my colleague from Texas for his attention to this issue. I fully support H.R. 4743, the National Cybersecurity Preparedness Consortium Act of 2016. I urge my colleagues to support this bill.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield 4 minutes to the gentleman from Texas (Mr. CASTRO), the author of this bill.

Mr. CASTRO of Texas. Mr. Speaker, I thank Ranking Member THOMPSON for yielding me this time and for his support of this legislation. He and his staff have been terrific partners in moving this bill forward.

I would also like to thank my fellow Texans, Chairman MCCAUL, Congressman HURD, Congressman RATCLIFFE, and also Congressman RICHMOND, who is not a Texan, but is a wonderful person here in our body, for all of their work on this issue.

Every day our Nation faces a growing number of potentially debilitating cyber threats. Our retailers, our banks, government agencies, military operations, and everyday private American citizens all face these threats. We must ensure that our defenses are as strong as possible because of that.

I represent San Antonio, a national leader in the cybersecurity field. Institutions in San Antonio do cutting-edge cyber work that keeps our Nation safe.

For example, the University of Texas at San Antonio leads the National Cybersecurity Preparedness Consortium, which helps communities across the Nation improve their cyber defenses.

It is critical that localities understand the impact cyber attacks could have on their ability to function and are prepared to prevent, detect, respond to, and recover from harmful cyber incidents.

UTSA and its cybersecurity consortium are educating communities about these cyber threats and helping them develop the defenses they need to successfully withstand a cyber emergency.

This legislation allows consortiums like UTSAs to work more closely with DHS to address cybersecurity risks and incidents at the State and local level. This collaboration will bolster our cyber preparedness and keep us one step ahead of cyber attackers.

Mr. Speaker, again I would like to thank the Homeland Security Committee's leadership for their partnership on this legislation and also all of the staff, both Republican and Democratic, who helped bring this to the floor.

Mr. RATCLIFFE. Mr. Speaker, I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, the inspiration for this bill was important work being done by the National Cybersecurity Preparedness Consortium, a group of five universities led by the University of Texas at San Antonio that has helped to raise cyber preparedness at the State and local level by evaluating communities, cybersecurity postures, and providing them with a roadmap to correct deficiencies.

While this consortium is making an important contribution to cybersecurity, there is an enormous need for training and technical assistance around the Nation. With the enactment of H.R. 4743, more institutions will be able to partner with DHS to provide such critical assistance.

As such, I urge passage.

I yield back the balance of my time.

Mr. RATCLIFFE. Mr. Speaker, I once again urge my colleagues to support H.R. 4743.

I yield back the balance of my time.

Mr. MCCAUL. Mr. Speaker, I rise in support of H.R. 4743, the National Cybersecurity Preparedness Consortium Act of 2016.

This bill allows the Department of Homeland Security to work with a cybersecurity consortium to carry out training, technical assistance and simulation exercises for State and local officials, critical infrastructure owners and operators and private industry.

The National Cybersecurity Preparedness Consortium, based at the University of Texas San Antonio's Center for Infrastructure Assurance and Security, provides research-based cybersecurity-related training and exercises to increase cybersecurity preparedness across the nation.

Other members of the Consortium include the Texas Engineering Extension Service in the Texas A&M University system, the University of Memphis, the University of Arkansas System, and Norwich University.

Last December, I helped usher through the landmark Cybersecurity Act of 2015. That legislation helps protect our nation's private sector and federal networks which are under continuous threat from foreign hackers and cyber terrorists. H.R. 4743 will be a value add in better securing the Nation's overall cybersecurity preparedness.

Locally, first responders and government officials as well as critical infrastructure owners and operators and private industry are bombarded with cybersecurity threats in the same way as at the federal level.

Helping organizations working to incorporate cybersecurity risk and incident prevention and response into State and local emergency plans is just one of the elements this bill encourages.

Allowing DHS to work with organizations like the Consortium, will ensure more tools are available back at home for those working to prepare for and combat cyber attacks on a regular basis.

I support this bill and urge my colleagues to do the same.

Ms. JACKSON LEE. Mr. Speaker, I rise in strong support of H.R. 4743, the National Cybersecurity Preparedness Consortium Act of 2016, because it will establish an important resource to ensure that private sector entities are better prepared to protect against cyber threats.

As a senior member of the House Committee on Homeland Security, I am well aware of the threats posed by cybersecurity vulnerabilities, and this bill takes an essential step to strengthen domestic cybersecurity.

H.R. 4743 establishes a National Cybersecurity Preparedness Consortium to engage academic, nonprofit, private industry, and federal, state, and local government partners to address cybersecurity risks and incidents, including threats or acts of terrorism.

The Consortium may provide training to State and local first responders and officials to equip them with the tools and skills needed to prepare for and respond to cybersecurity risks and incidents, including threats and acts of terrorism, in accordance with current law.

I thank both Chairman MCCAUL and Ranking Member THOMPSON for the bipartisan work done to bring the bill before the House for Consideration.

I am pleased that during the Committee markup of H.R. 4743, two important Jackson Lee Amendments were adopted.

The first Jackson Lee Amendment to H.R. 4743 establishes metrics as a measure of the effectiveness of the National Cybersecurity Preparedness Consortium program.

Having the information provided by my amendment to H.R. 4743, will allow the Congressional oversight committees to better plan future programs around cybersecurity collaborations that are intended to share knowledge on best practices in securing computer networks from attack.

The second Jackson Lee Amendment added an additional objective of the bill, a directive that should help participants prepare to address continuity of operations.

This amendment provides a focus for the Consortium's work on the issue of continuity of operation, which addresses whether an entity can survive a cyber-attack, continue to provide information or services during an attack; or the likelihood that the time to recovery from a successful cyberattack or threat is predictable and reasonable.

Just as the attacks on the morning of September 11, 2001 came without notice so may a major cyber-attack.

In March, of this year, U.S. Attorney General Lynch announced ''wanted'' notices for a group of Iranian hackers the United States believes are behind a 2013 computer intrusion of a small New York dam and a series of cyberattacks on dozens of U.S. banks.

There are many companies offering continuity of operations services to companies large and small with the intent that they will be there to support their clients in the event of a cyber incident.

The work of the Consortium should go beyond planning to the answering questions regarding the operationalization of plans in the event of an attack or cyber incident.

We know that planning is crucial, but we must encourage cybersecurity planning to go beyond the planning process to understand the capacity of an entity's continuity of operations plans by looking at continuity of operations of service providers should an incident impact an area or industry.

I support H.R. 4743, because it provides this assurance by providing critical cybersecurity collaboration among experts and industries that are essential to critical infrastructure operations or have a significant economic presence in our nation's economy that a cyber-attack would have broad repercussions.

I ask my colleagues to join me in supporting H.R. 4743.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. RATCLIFFE) that the House suspend the rules and pass the bill, H.R. 4743, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. RATCLIFFE. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this motion will be postponed.

DEPARTMENT OF HOMELAND SECURITY STRATEGY FOR INTERNATIONAL PROGRAMS ACT

Mr. RATCLIFFE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4780) to require the Secretary of Homeland Security to develop a comprehensive strategy for Department of Homeland Security operations abroad, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4780

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Department of Homeland Security Strategy for International Programs Act''.

SEC. 2. COMPREHENSIVE STRATEGY FOR INTERNATIONAL PROGRAMS FOR VETTING AND SCREENING PERSONS SEEKING TO ENTER THE UNITED STATES.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a comprehensive three-year strategy for international programs of the Department of Homeland Security in which personnel and resources of the Department are deployed abroad for vetting and screening of persons seeking to enter the United States.

(b) CONTENTS.—The strategy required under subsection (a) shall include, at a minimum, the following: